



# **ICAM Privileged User Instruction and Implementation Guidance**

**Version 1.0**

**October 15, 2014**

This page is intentionally left blank.

## Authority

This document has been developed by the Privileged User Tiger Team (PUTT) of the Identity, Credential, and Access Management Subcommittee (ICAMSC), as supplemental guidance to the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.<sup>1</sup> The ICAMSC was established in 2008 by the Federal Chief Information Officers (CIO) Council's Information Security and Identity Management Committee (ISIMC) and was tasked with aligning the Identity Management activities of the Federal Government. The development of this document aligns with and supports the responsibilities of the ICAMSC, which include:

- Aligning federal agencies around common practices by fostering effective government-wide Identity, Credential, and Access Management (ICAM);
- Collaborating with Federal Government and external identity management activities (non-federal, commercial, and more) to leverage best practices and enhance interoperability; and
- Enabling trust and interoperability in online transactions, through the application of common policies and approaches, in activities that cross organizational boundaries.

This guidance has been prepared for use by federal agencies and is not intended to contradict other previously established standards and guidelines that are mandatory and binding on federal agencies. Additionally, these guidelines should not be interpreted as altering or superseding the existing authority of the FICAM Roadmap.

---

<sup>1</sup> [Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance](#), Version 2.0, Federal Chief Information Officers Council, December 2, 2011, [FICAM Roadmap].

This page is intentionally left blank.

## Executive Summary

The President released the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*<sup>2</sup> (NITP) in 2012 to address the need for federal agencies to monitor all employees who may pose a threat to national security. In particular, recent incidents highlighted the need for improved management of privileged users within the Federal Government. These incidents involved employees or contractors with elevated access wrongfully exposing information due to a lack of effective access control, which in many cases allowed them unrestricted access to agency information systems. These incidents compromised national security by exposing sensitive information as well as damaging the reputation of affected agencies.

Certain individuals need elevated access to perform necessary administrative and security functions for federal agencies, yet this carries an inherent risk of misuse or abuse. As a result, agencies should implement controls for privileged users that mitigate unwanted behavior, without impeding their ability to carry out assigned job duties. In creating a secure physical and virtual workplace for privileged users, agencies should align efforts with Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM Roadmap).<sup>3</sup>

This document provides federal agencies with guidance to manage its privileged users by mitigating the inherent risks associated with this population through the use of Identity, Credential, and Access Management (ICAM). In summary, nine primary steps are suggested for an agency to improve its privileged user risk management:

1. Identify and document mission critical and sensitive resources.
2. Identify the individuals and accounts that interact with mission critical and sensitive resources.
3. Identify the individuals that require elevated access to the protected resources.
4. Conduct a risk assessment by analyzing vulnerabilities, impact, and likelihood of misuse or abuse of elevated access by privileged users.
5. Develop a secure operating environment for the privileged user population.
6. Execute effective provisioning of privileged users.
7. Implement run-time access control using privileged user management techniques.
8. Perform on-going monitoring of privileged users at a level commensurate to the risk posed.

---

<sup>2</sup> [Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs](#), Office of the Press Secretary, November 21, 2012. [NITP]

<sup>3</sup> [Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance](#), Version 2.0, Federal Chief Information Officers Council, December 2, 2011, [FICAM Roadmap].

**9. Consult leading information security guidance on methods to further improve privileged user management throughout the enterprise.**

As further detailed within this document, it is crucial that an agency identify which individuals have elevated access to an agency's protected resources (Steps 1 – 3). Once the scope of privileged users' interactions with protected resources (Step 4) is understood by the agency, it should leverage the Privileged User Management Framework outlined within this document to mitigate the risk of these users engaging in unwanted behavior (Steps 5 – 8). Implementing standard mechanisms within ICAM best practices as well as additional countermeasures to prevent privileged user misuse or abuse of elevated access can provide comprehensive, integrated protection for agency resources. Steps 5 – 8 should operate in unison; however, they are presented in a logical progression. Furthermore, an agency can bolster the activities within the Privileged User Management Framework by leveraging existing efforts to achieve information security goals by directing or tailoring these activities based on its resources, environment, mission, business needs, and privileged user population (Step 9). To assist in this effort, this document includes a collection of useful references, insider threat classifications, and a security controls mapping to the National Institute for Standards and Technology's Special Publication 800-53.<sup>4</sup>

---

<sup>4</sup> [SP 800-53](#), Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST, April 2013. [SP 800-53]. For agencies operating on classified fabrics, please leverage [Security Categorization and Control Selection 1253](#) (CNSS 1253), as this document identifies applicable options in alignment with SP 800-53.

## Table of Contents

<b>Authority .....</b>	<b>iii</b>
<b>Executive Summary .....</b>	<b>v</b>
<b>Table of Contents .....</b>	<b>vii</b>
<b>List of Figures .....</b>	<b>viii</b>
<b>1. Introduction .....</b>	<b>1</b>
1.1. Background .....	1
1.2. Purpose .....	2
1.3. Scope .....	2
1.4. Assumptions .....	3
1.5. Reference Documentation .....	3
<b>2. Privileged User Landscape Overview .....</b>	<b>5</b>
2.1. Unwanted Behavior by Privileged Users .....	6
2.2. Evaluating Privileged User Risks .....	6
<b>3. Privileged User Management Framework .....</b>	<b>9</b>
3.1. Secure Operating Environment .....	11
3.2. Provisioning .....	13
3.3. Run-Time Access Control .....	15
3.4. On-Going Monitoring .....	17
<b>Appendix A: Reference Documentation .....</b>	<b>19</b>
<b>Appendix B: Classifications of Insider Threats and Privileged Users .....</b>	<b>25</b>
<b>Appendix C: Privileged User Security Controls Mapping for Special Publication 800-53 .....</b>	<b>27</b>
<b>Appendix D: Privileged User Instruction .....</b>	<b>41</b>

## List of Figures

Figure 1: Unwanted Behavior by Privileged Users .....	6
Figure 2: Example Set of Elevated Access Profiles for a Resource .....	8
Figure 3: Privileged User Management Framework .....	10
Figure 4: Protected Resource Definitions .....	15
Figure 5: Classifications of Insider Threat and Privileged Users .....	26
Figure 6: Access Control .....	28
Figure 7: Awareness and Training .....	29
Figure 8: Audit and Accountability .....	30
Figure 9: Security Assessment and Authorization .....	31
Figure 10: Configuration Management .....	32
Figure 11: Contingency Planning .....	33
Figure 12: Identification and Authentication .....	33
Figure 13: Incident Response .....	34
Figure 14: Maintenance .....	35
Figure 15: Media Protection .....	35
Figure 16: Physical and Environmental Protection .....	36
Figure 17: Planning .....	36
Figure 18: Personnel Security .....	38
Figure 19: Risk Assessment .....	38
Figure 20: System and Services Acquisition .....	39
Figure 21: System and Communications Protection .....	40
Figure 22: System and Information Integrity .....	40



# 1. Introduction

## 1.1. Background

In alignment with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM Roadmap),<sup>5</sup> federal agencies are responsible for ensuring that their employees and contractors are fulfilling their job functions through appropriate use of the physical and logical resources to which they have access. In recent years, the Federal Government has experienced incidents in which an individual employee or contractor with elevated access<sup>6</sup> compromised security from within agency boundaries. In some instances, these individuals were able to expose content and data due to a lack of effective access control, which allowed them unrestricted access to information systems.

In 2012, the President released the “*National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*,”<sup>7</sup> (NITP) to address the need for federal agencies to monitor all employees who may pose a threat to national security. Additionally in 2012, the *National Strategy for Information Sharing and Safeguarding* (NSISS) was released, in which one of its highlighted goals supports identifying, preventing, and mitigating insider threats to the Federal Government.<sup>8</sup> As a result of the NITP, NSISS, and federal security incidents, agencies have begun to develop policy, regulations, and programs that mitigate unwanted actions (e.g., espionage, disclosure of information) by employees, including privileged users.<sup>9</sup> In order to proactively mitigate these threats, the NITP requires agencies to:

- Gather, integrate, and centrally analyze and respond to key threat-related information;
- Monitor employee use of classified networks;
- Provide the workforce with insider threat awareness training; and
- Protect the civil liberties and privacy of all personnel.<sup>10</sup>

In particular, these employees and contractors who require elevated access to facilities and information systems to fulfill their organizational role (i.e., privileged users) have the ability to jeopardize sensitive information or infrastructure, whether knowingly or unknowingly. Administrative and security related functions commonly assigned to privileged users grant these individuals the means to compromise all three core elements of information security: availability, confidentiality, and integrity.<sup>11</sup> Therefore, an attack executed by a privileged user can have

---

<sup>5</sup> [Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance](#), Version 2.0, Federal Chief Information Officers Council, December 2, 2011, [FICAM Roadmap].

<sup>6</sup> Elevated access allows a user to perform security or administration functions on a protected resource that the general user population is not authorized to perform. Individuals who are granted elevated access are referred to as privileged users. Refer to Section 2 for the definition of a privileged user.

<sup>7</sup> “[Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs](#),” Office of the Press Secretary, November 21, 2012. [NITP]

<sup>8</sup> [National Strategy for Information Sharing and Safeguarding \(NSISS\)](#), Executive Office of the President (EOP), December 2012. [NSISS]

<sup>9</sup> Please see Section 2 for the definition of a privileged user.

<sup>10</sup> [NITP](#)

<sup>11</sup> [FIPS 199](#), Standards for Security Categorization for Federal Information and Information Systems, National Institute of Standards and Technology (NIST), April 2004. [FIPS 199]

especially damaging effects on a federal agency. The threat posed by privileged users demonstrates the need for a concerted federal effort to manage these essential, yet inherently risky, individuals through policy-based and technical measures.

Privileged users have been responsible for the most recent high-profile federal security breaches since the release of NITP, bolstering the need for agencies to align with the requirements outlined in NITP, and in particular, emphasizing the management of their privileged user populations. As part of the insider threat program required by NITP, agencies should focus on developing stringent policy to proactively address the threat privileged users can pose from within. Relevant activities would address the three federal requirements of agencies: mitigate the insider threat, protect agency operations, and safeguard sensitive information.

In support of this need, the Identity, Credential, and Access Management (ICAM) Sub-Committee (ICAMSC) within the Information Security and Identity Management Committee (ISIMC) of the Federal Chief Information Officer (CIO) Council directed the development of a Privileged User Instruction (i.e., privileged user agreement) and Implementation Guidance. Agencies should work to proactively, securely, and efficiently manage their privileged user populations in alignment with the FICAM Roadmap. To support agencies in overcoming the challenges associated with privileged user management, the ICAMSC formed the Privileged User Tiger Team (PUTT). This group has been tasked with developing guidance that provides instruction and implementation best practices to federal agencies for managing and monitoring privileged users across security domains. The PUTT has collaborated with several agencies to provide leading practices for monitoring, identifying, and mitigating potential threats to agency resources to maintain control of agency data and drive security improvements across the federal enterprise.

## **1.2. Purpose**

The purpose of this document is to provide guidance to federal agencies to assist in managing their privileged users' access to agency protected resources (i.e., content and data, applications and web services, network and infrastructure, facilities). This document will serve as a supplement to the FICAM Roadmap<sup>12</sup> and *Committee on National Security Systems (CNSS) Directive 504 Annex C*<sup>13</sup> by providing guidance for managing privileged users that is applicable across security domains.

## **1.3. Scope**

The scope of this document is limited to high-level guidance that is specific to privileged users accessing operational Federal Government information systems and physical resources across security domains. This document is not to supersede existing policy or requirements.

The following items fall outside the scope of this document:

- Recommendations and guidance specific to only one security domain (i.e., unclassified, Secret, Top Secret);

---

<sup>12</sup> [FICAM Roadmap](#)

<sup>13</sup> See the [CNSS website](#) for CNSS directives, issuances, and policies.

- Timelines associated with achieving the leading management approaches and practices outlined herein; and
- Implementation of an agency's insider threat program as it relates to privileged users in fulfillment of NITP requirements.

## 1.4. Assumptions

This document takes into consideration the following assumptions and dependencies:

1. The information in this document is based upon information, knowledge, and analysis provided by the participating agencies in the tiger team and public comment period.
2. The leading management approaches and practices highlighted within this document include interim measures that agencies have implemented to manage privileged users in support of achieving the desired target state.
3. The information in this document is not to supersede guidance provided for national security systems via CNSSD 504 Annex C.
4. The information in this document supports the requirement and assumes that an agency has implemented National Institute for Standards and Technology's (NIST) *Special Publication 800-53: Security and Privacy Control for Federal Information Systems and Organizations* (SP 800-53),<sup>14</sup> per the *Federal Information Security Management Act* (FISMA).<sup>15</sup>

## 1.5. Reference Documentation

There are a variety of policies and standards that bind federal agencies to the national effort of protecting the country against insider threat. Taken together, these documents communicate the urgency for federal agencies to implement proper controls for privileged users, because they pose a heightened risk to their respective organizations and the country at large. Documents outlined in Appendix A: Reference Documentation, include the National Insider Threat Policy (NITP),<sup>16</sup> relevant Executive Orders (E.O.), FISMA, the *Standards for Security Categorization for Federal Information and Information Systems* (FIPS 199),<sup>17</sup> FICAM Roadmap,<sup>18</sup> and SP 800-53,<sup>19</sup> and the Software Engineering Institute at Carnegie Mellon's Insider Threat Center's *Common Sense Guide to Mitigating Insider Threats* (4<sup>th</sup> Edition).<sup>20</sup>

---

<sup>14</sup> [SP 800-53](#), Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST, April 2013. [SP 800-53]

<sup>15</sup> [FISMA Metrics](#), FY2014 Chief Information Office Federal Information Security Management Act Reporting Metrics v2.0, January 2014. [FISMA Metrics]

<sup>16</sup> [NITP](#)

<sup>17</sup> [FIPS 199](#)

<sup>18</sup> [FICAM Roadmap](#)

<sup>19</sup> For agencies operating on classified fabrics, leverage [CNSS 1253](#).

<sup>20</sup> [Common Sense Guide to Mitigating Insider Threats \(4<sup>th</sup> Edition\)](#), CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University, December 2012. [Common Sense Guide]

This page is intentionally left blank.

## 2. Privileged User Landscape Overview

An agency is responsible for managing the privileges of all users with access to agency resources to ensure that employees can fulfill their assigned duties efficiently and securely.<sup>21</sup> To execute assigned duties, a subset of an agency's user population may be granted elevated access to an agency's protected resources (e.g., content and data, applications and web services, network and infrastructure, facilities), which if misused or abused, could significantly compromise these resources.<sup>22</sup> The individuals entrusted with elevated access constitute an agency's privileged user population.

### Terminology

**Privileged User** – A user who has been granted elevated privileges for access protected physical or logical resources. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared information technology (IT) infrastructure, and require access to related systems to create new user accounts, and add to or amend the privileges of other users.<sup>23</sup>



An agency's privileged user population can include a range of individuals entrusted with elevated access. For example, both a security guard with physical access to a server room and a UNIX administrator with root access may be categorized as privileged users, despite different elevated access profiles. Given the broad-reaching nature of an organization's privileged user population, it is important that an agency understand the user groups and accounts that constitute its privileged user population. Examples of individuals who may be considered privileged users include: application developer, database administrator, data center operations personnel, information technology (IT) security practitioner, IT audit practitioner, maintenance personnel, network engineer, and system administrator. Because of privileged users' elevated access, unwanted behavior by these individuals can significantly compromise agency assets or operations. As a result, privileged user management is a cornerstone of insider threat mitigation.

---

<sup>21</sup> Referred to as "privilege management;" the definition can be found in the [FICAM Roadmap](#).

<sup>22</sup> Please see Section 3.3 for information on protected resources.

<sup>23</sup> This definition is derived from the FY14 FISMA Metrics, as defined in the [Information Security Glossary](#).

## 2.1. Unwanted Behavior by Privileged Users

Since misuse or abuse of elevated access can significantly compromise an agency's protected resources, the agency should be fully aware of the potential for privileged users to exploit their organizational roles. The responsibilities (e.g., audit, maintenance, configuration) commonly assigned to privileged users and the level of access they maintain (e.g., operating systems, virtual directories, web services and applications, databases), render protected resources vulnerable to privileged users who do not act in accordance with security protocol. The exploitation of elevated access to protected resources by privileged users may involve a variety of unwanted behaviors (e.g., fraud, sabotage) as outlined in Figure 1. This unwanted behavior can lead to catastrophic events, such as a privileged user with broad access to agency files for administrative purposes copying classified files on portable media.

Unwanted Behavior	Definition	Examples of Unwanted Behavior by Privileged Users
<b>Fraud</b>	Unwanted use, modification, addition, or deletion of agency's data for personal gain.	On the pretense of fixing corrupt data, a database administrator modifies data without authorization.
<b>Espionage</b>	Sharing restricted information with the intention of aiding a foreign actor or harming the U.S. Government.	System administrator uses elevated access to retrieve confidential data and sells it to a foreign actor.
<b>Sabotage</b>	Purposefully inflicting harm on an organization.	Maintenance worker inserts a Universal Serial Bus (USB) drive into a server to inject malware on behalf of an external bad actor.
<b>Intellectual Property Theft</b>	Stealing intangible assets (e.g., discoveries, inventions, designs) from an organization.	Cloud administrator uses elevated access to server to steal proprietary information.
<b>Unwanted Information Disclosure</b>	A communication or physical transfer of information to a recipient who is not authorized to access to the information.	System administrator creates a "backdoor" account to inappropriately access and release classified information.

Figure 1: Unwanted Behavior by Privileged Users

## 2.2. Evaluating Privileged User Risks

As the first step in mitigating privileged users' engaging in the unwanted behavior described in Figure 1, an agency should evaluate the risks to its protected resources by leveraging its resource risk assessment as required<sup>24</sup> in addition to a user community analysis.<sup>25</sup> These processes are components of a protected resource analysis, a foundational element of safeguarding agency resources (see Figure 4). For more information on how to conduct a comprehensive protected resources analysis, refer to the Access Management Framework.<sup>26</sup> In combination, a resource risk assessment and a user community analysis allows an agency to identify its privileged user population and related risks to protected resources. It is recommended that an agency follow these steps to identify its privileged users:

<sup>24</sup> [FIPS 199](#)

<sup>25</sup> "User community" is terminology derived from the Access Management Framework (AMF). For the purpose of the Privileged User Instruction and Implementation Guidance, this term is used synonymously with "user population." (Hyperlink to be provided once publicly available).

<sup>26</sup> For more information on risk assessments for protected resources, refer to the AMF. (Hyperlink to be provided once publicly available).

1. Identify and document mission critical and sensitive resources (Figure 4).
2. Identify the individuals and accounts that interact with mission critical and sensitive resources, with the understanding that some individuals may have elevated access that their current job functions do not require, and vice versa.
3. Identify the individuals that require elevated access to the protected resources. These individuals constitute an agency's privileged user population. As part of this process, agencies should identify these individuals' roles and the frequency with which these roles change. Based on these determinations, an agency should provision and de-provision elevated access as necessary in support of a user's job function and role. This activity is outlined in Section 3.2.

#### Implementation Tip

When identifying an agency's privileged user population, it is important to validate that the elevated access an individual possesses supports his/her job function. If the elevated access is not needed, it should be immediately revoked and de-provisioned. De-provisioning is performed when there is a need to permanently eliminate an existing access permission or remove a user account altogether.



Once an agency identifies its privileged user population for a protected resource, it can analyze the related vulnerabilities, impact, and likelihood of misuse or abuse.<sup>27</sup> An agency can then categorize these privileged users into groups based on their job functions and types of privileges (i.e., logical, physical).<sup>28</sup> Using these groups, an agency can allocate resources to manage privileged users at a level commensurate with the associated risks

The following table provides examples of job functions that may have elevated access to agency resources. As an agency advances its enterprise-wide access control services, and thus its convergence of physical and logical access activities and processes, it may have job functions with elevated access that overlap both logical and physical resources (as highlighted below).

Job Functions	Examples of Elevated Access
<b>Application Administrator</b>	<ul style="list-style-type: none"> <li>Access to logical information is controlled through a variety of managed application interfaces; however, the user is granted additional privileges within the constraints of the application interface.</li> <li>Physical access to organization-specific sensitive doors or turnstiles that do not contain shared systems or infrastructure.</li> </ul>
<b>System Administrator</b>	<ul style="list-style-type: none"> <li>User has elevated or complete access to one or more vertical systems or applications. Compromise to a system is limited to the application-specific capabilities, and loss of availability would not impact the entire organization.</li> <li>A Non-Person Entity (NPE) has access to communicate and otherwise interact with other systems within an application vertical. Damage from the compromise of an NPE's account is limited to the application vertical.</li> <li>Physical access to organization-specific sensitive doors or turnstiles that do not contain shared systems or infrastructure.</li> </ul>

<sup>27</sup> For more information on the basis for privileged users' unwanted behavior, refer to Appendix B: Classifications of Insider Threats and Privileged Users.

<sup>28</sup> For more information on logical and physical access control systems, refer to the [FICAM Roadmap](#).



Job Functions	Examples of Elevated Access
<b>Shared Infrastructure Administrator</b>	<ul style="list-style-type: none"> <li>User has elevated or complete access to one or more shared systems, applications or infrastructure. Compromise of these systems could impact large portions of or the entire organization.</li> <li>An NPE has access to communicate and otherwise interact with other shared infrastructure systems. Damage from the compromise of an NPE's account could impact large portions of or the entire organization.</li> <li>Physical access to doors or turnstiles protecting critical shared infrastructure, information, or other physical resources. Compromise of these physical controls could result in multiple types of wide-spread damage to the organization's physical and logical resources.</li> </ul>

**Figure 2: Example Set of Elevated Access Profiles for a Resource**

By granting privileged users elevated access to protected resources, an agency becomes vulnerable to the risk of a privileged user misusing or exploiting these resources out of accidental, complacent, or malicious behavior.<sup>29</sup> The management requirements developed from assessing a resource's privileged user population and associated privileged accounts can serve as core factors for federal agencies to consider when selecting, implementing, and configuring mechanisms to mitigate unwanted behavior by privileged users. These mechanisms should include detective and preventive measures to provide a holistic approach to privileged user management.

#### FAQ

##### **What is the difference between preventive and detective measures?**

Preventive measures seek to proactively inhibit inappropriate behavior through measures such as background investigations, training, etc. Detective measures serve to identify unusual, suspicious behavior or changes in activity to proactively mitigate risk to agency facilities and resources (e.g., keystroke logging, audit logs). An agency should leverage both preventive and detective measures for privileged user activities.



An agency should seek to leverage existing processes and controls to effectively manage its privileged user population and protected resources. Please refer to Appendix C: Privileged User Security Controls Mapping for Special Publication 800-53 for a mapping of controls defined in SP 800-53. These controls have been augmented to serve as countermeasures for how an agency can mitigate unwanted behavior by its privileged user population.

#### FAQ

##### **What if my agency discovers privileged accounts that are not associated with one person during a protected resource analysis?**

Conducting a protected resource analysis allows an agency to identify the privileged accounts relevant to protected resources. An agency may discover privileged accounts that lack accountability as they are not associated with one person, including orphaned, rogue, and default accounts that have gone unnoticed or unmanaged. Once these problematic accounts are identified, an agency can determine whether these accounts should exist, and if so, which accountability mechanism should be applied (e.g., assign administrator).



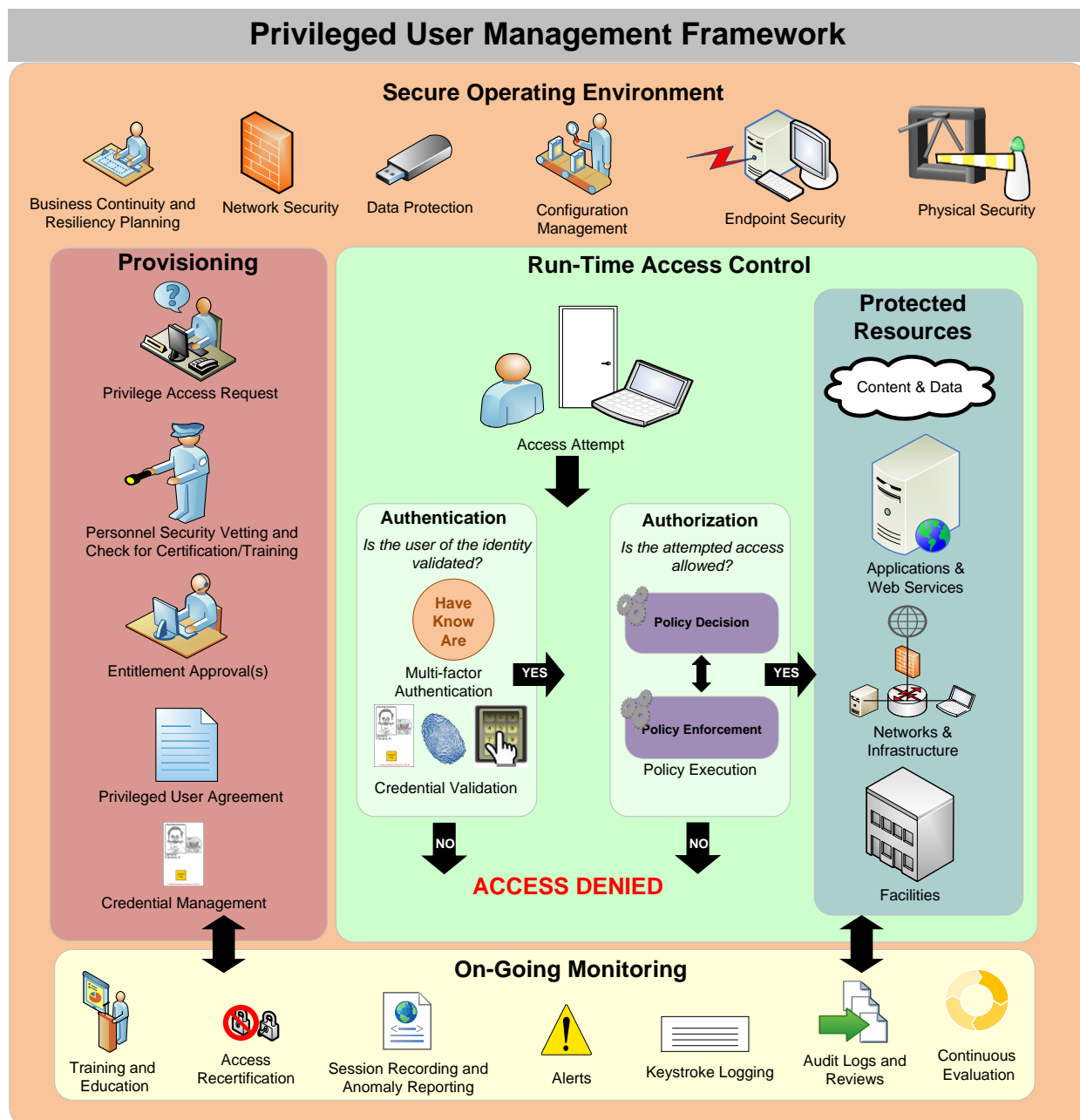
<sup>29</sup> For more information on the basis for privileged users' unwanted behavior, refer to Appendix B: Classifications of Insider Threats and Privileged Users.



### **3. Privileged User Management Framework**

As discussed in Section 2, there may be a variety of privileged users that constitute an agency's privileged user population with an assortment of elevated access profiles. An agency can use a protected resource analysis to determine the risk associated with each elevated access profile, which can guide the implementation of a range of preventive and detective measures. To improve the management of the privileged user population using these measures, an agency should leverage a repeatable process, because it allows an agency to track and monitor privileged user activity and job functions with consistency, thereby enforcing security protocol and detection abilities. Accordingly, an agency should consider implementing the following Privileged User Management Framework to mitigate the risk of privileged users committing the unwanted behaviors described in Section 2.1. This framework offers an overview of a standard set of mechanisms, or countermeasures, to manage an agency's diverse privileged user population, so that protected resources are safeguarded and security protocol is followed.

As an agency looks to proactively manage its privileged user population, leveraging the Privileged User Management Framework illustrated in Figure 3 can support these efforts.



**Figure 3: Privileged User Management Framework**

The framework represents a cohesive set of measures to manage privileged users and to assist in holistically protecting the enterprise. First, an agency should have the elements of a Secure Operating Environment for privileged user activities in place in order to effectively support the subsequent privileged user management techniques. Without a Secure Operating Environment, an agency does not have the proper groundwork to support the remaining processes and measures in the Privileged User Management Framework. Implementing preventive measures geared towards privileged users, such as firewalls, secure remote access, and file restrictions can support an agency in securing its IT environment so privileged users are controlled and monitored effectively.

The Privileged User Management Framework includes provisioning of the privileged user. Provisioning refers to creating user accounts and assigning privileges or entitlements within the scope of a defined process or interaction to provide users with access rights to applications and other resources that may be available in an environment.<sup>30</sup> Provisioning activities assist an agency in managing how elevated access is assigned to privileged users and maintaining central situational awareness regarding which privileged users have what kind of access to protected resources.

When the privileged user obtains a credential required for access, the privileged user attempts to use his/her elevated access via run-time access control to interact with one of the four protected resources (i.e., content and data, applications and web services, network and infrastructure, facilities). To access the protected resource(s), the privileged user must successfully authenticate in order for an affirmative authorization decision to be made.<sup>31</sup> An agency can hold privileged users to a higher authentication standard than standard users because of the higher risk associated with elevated access. On-going monitoring of privileged user activity can verify that these users' activities are in line with the job function or a business purpose to help discern valid actions from malicious, careless, and accidental actions.

The following subsections provide a more detailed discussion of each piece of the Privileged User Management Framework.

### **3.1. Secure Operating Environment**

A Secure Operating Environment includes controls (e.g., firewalls, secure remote access, file restrictions) to protect the agency's IT infrastructure (e.g., business applications, devices, data), which privileged users leverage to carry out job functions.<sup>32</sup> The following activities encompass a host of processes and controls which, when taken together, build a Secure Operating Environment to enable privileged user management techniques in the rest of the framework:

- 1. Business Continuity and Resiliency Planning.** Improper use of privileged users' elevated access to critical agency resources can cause disruptions such as system failures, outages, or data loss, whether through either intentional or accidental means. Sustaining an organization's mission and business operations during and after disruption requires established continuity and resiliency plans, processes, and technology. This can include continuity of operations (COOP) plans, data backup, alternate operating sites, secure recovery processes, etc.
- 2. Network Security.** An agency can prevent unwanted access, misuse, or modification of a computer network through the use of firewalls, intrusion detection, secure remote access, etc. In particular, an agency can configure these mechanisms to manage the privileged user population. For example, an agency can configure firewalls to restrict access to privileged user accounts using an IP address and can configure remote access to restrict the execution of privileged commands via remote access.

---

<sup>30</sup> As defined in the [FICAM Roadmap](#).

<sup>32</sup> An agency should conduct recurring training for its users on how to protect the agency's IT infrastructure as part of On-going Monitoring, described in Section 3.4.

3. **Data Protection.** For administrative or security reasons, a privileged user may have access to a large amount of sensitive information, necessitating protective mechanisms for such data. Enforcing restrictions and tight controls over data assists in safeguarding information in transit. Implementing mechanisms such as encryption, exfiltration controls, and file size restrictions assists in secure exchanges of information and relevant data that a privileged user may handle in support of his/her job function.
4. **Configuration Management.** Maintaining the performance level and attributes of an information system to match mission requirements entails managing the system's configurations. Developing stringent controls and accountability mechanisms for establishing a secure configuration baseline, approving configuration changes, and validating configuration compliance assist an agency in protecting its system from unwanted modifications and use. As part of configuration management, an agency should consider enforcing the use of approved software (i.e., blacklisting [unwanted software], whitelisting [authorized software]) and maintaining appropriate patching of configuration levels to defend privileged user credentials when these users perform security and administration functions.
5. **Endpoint Security.** Endpoint security ensures all devices on a network meet predetermined standards before access to the network is granted. This approach to network security allows an agency to defend its protected resources from individuals who are not authorized to have elevated access. An agency should equip devices accessed by privileged users with the appropriate security configurations (e.g., anti-malware) in order to defend privileged user accounts and credentials from compromise.
6. **Physical Security.** Physical security protects employees, data, and information technology infrastructure from harm. However, users with elevated physical access can undermine the efficacy of strong IT controls for resources in protected physical spaces. To manage physical activity, an agency can use an IT-enabled physical access control system (PACS) that is integrated with capabilities such as video surveillance, guard force, notification systems, and fire alarms. To safeguard protected resources, an agency should integrate its physical and network security processes and technologies through access control convergence.<sup>33</sup>

As an agency determines the appropriate controls to implement in its Secure Operating Environment, it is important to consider the number of controls and related requirements. Implementation of unnecessary controls can create management repercussions such as costly and time consuming maintenance and cumbersome management and oversight.

## FAQ

### How can an agency mitigate unwanted behavior by complacent privileged users?

In addition to training and education, an agency can address complacent insider activity by implementing internal controls and processes, such as software blacklisting and whitelisting, segregation of duties, checking passwords in and out, etc. The Privileged User Management Framework includes a host of internal controls and processes to protect the enterprise from a careless privileged user.



<sup>33</sup> For more information on physical and logical access control convergence, refer to Section 9 of the [FICAM Roadmap](#).

### 3.2. Provisioning

As discussed in Section 3 the provisioning portion of the framework is multi-faceted and determines who within the enterprise should have elevated access based on job function, business need, and background of the user. An agency should only grant entitlements that the privileged user needs to perform assigned duties by leveraging segregation of duties<sup>34</sup> and the “principle of least privilege.”<sup>35</sup> At a minimum, an agency should include the following activities when conforming to this portion of the Privileged User Management Framework:

1. **Privilege Access Request.** An individual completes a request for access to an application and provides it to the individual responsible for access approvals.<sup>36</sup>
2. **Personnel Security Vetting and Check for Certification/Training.** The Personnel Security Office verifies that the existing background, suitability or fitness checks are valid and adequate. When conducting these checks, an agency should implement a consistent approach that enforces background checks that are commensurate to the privileged user’s level of risk as determined by an agency’s risk assessment, as outlined in Section 2.2.
3. **Entitlement Approval(s).** The individual responsible for approving the privileged user validates the individual’s need for access. A user account for the privileged user is then created with the appropriate user entitlements.
4. **Privileged User Agreement.** The privileged user reads and understands the agency’s privileged user agreement. This agreement highlights the responsibilities of the privileged user and acceptable rules of behavior. See Appendix D: Privileged User Instruction for a sample agreement template. An agency’s Privileged User Agreement may include a training requirement for the privileged user to fulfill prior to beginning executing the job functions that require elevated access.

#### Implementation Tip

Documenting a privileged user’s acknowledgement of his/her role and responsibilities is an excellent way to formalize the privileges granted. Implementing a standard privileged user acknowledgement form that requires the individual’s signature reinforces the privileged user’s responsibilities and helps the agency maintain a record indicating acknowledgement.



5. **Credential Management.** Leveraging secure, unique credentials (i.e., Personal Identity Verification card [PIV card])<sup>37</sup> is both a preventive and detective measure for managing privileged users and aligns with the ICAM target state. PIV cards allow an agency to improve monitoring of privilege user activity versus a credential that is neither unique nor differentiated from those of other privileged users (e.g., shared

<sup>34</sup> Defined in the [FICAM Roadmap](#) as a manual process for granting entitlement across applications and resources to determine if access entitlements violate policies. Per SP 800-53, an agency should not allow a single individual to perform the processing, adjudication, and provisioning of elevated access.

<sup>35</sup> Defined in the [FICAM Roadmap as the principle by which](#) users are only authorized to access whatever is needed to perform their jobs.

<sup>36</sup> Per the [FICAM Roadmap](#), Section 4.7.

<sup>37</sup> For the purpose of this document, the Personal Identification (PIV) Card and Common Access Card (CAC) are used synonymously.

username/password).<sup>38</sup>

In response to HSPD-12 and OMB M-11-11,<sup>39</sup> agencies have made a significant investment in the PIV card, which employees and contractors must use when authenticating to logical resources. Additionally, agencies have invested in the supporting infrastructure for PIV cards, enabling more secure physical and logical access control. Leveraging the existing PIV infrastructure to manage privileged user authentication provides an agency with enhanced security, reduced risk, and decreased cost relative to issuing alternative credentials (e.g., tokens, username/password).<sup>40</sup>

However, in standing up this PIV infrastructure, agencies had to manage versions of various operating systems that did not support the mapping of a single PIV card to multiple accounts. As agencies migrate to PIV-enabled technologies for privileged user accounts that support a seamless login experience (i.e., single sign-on),<sup>41</sup> leveraging secure credentials during this transition period is imperative. In order to satisfy requirements based on a system's security categorization and level of assurance<sup>42</sup> during this transition, an agency can leverage the PIV infrastructure to support issuance of a second credential for systems that do not currently support PIV authentication.<sup>43</sup> For example, a protected resource may require the use of username/password for system accounts in order for privileged users to perform administrator functions. Because username/password provides a lower level of assurance than the PIV card, an agency should have the appropriate controls in place to manage the increased risk. A leading practice in managing username/password for privileged users is a check-in/check-out capability, often referred to as a password vault. A password vault authenticates the privileged user so that he/she can select the account and password that is needed. The password is checked back into the vault once the privileged user's session on the shared/group account ends, providing the agency with more control over the use of passwords by privileged users. An agency should only use a password vault if its privileged users authenticate to the vault with the PIV card and if it is pursuing technologies that support PIV-enablement of privileged user accounts.

---

<sup>38</sup> Per the [FICAM Roadmap](#), it is anticipated agencies will experience a transition period in working to modernize systems to meet the requirements of the ICAM target state. Please refer to Section 8.3.3 of the [FICAM Roadmap](#) for recommended transition activities to manage privileged users' PIV cards and associated infrastructure.

<sup>39</sup> [M-11-11](#), Continued Implementation of Homeland Security Presidential Directive (HSPD) -12-Policy for a Common Identification Standard for Federal Employees and Contractors, OMB, February 3, 2011. [M-11-11]

<sup>40</sup> As discussed in Section 8.3.3 of the [FICAM Roadmap](#), an agency should not stand up a new alternative credential infrastructure if one is not already in place.

<sup>41</sup> Single sign-on is the mechanism by which a single act of user authentication and log on enables access to multiple independent resources as defined in the [FICAM Roadmap](#).

<sup>42</sup> Also referred to as Assurance Level. Level of assurance is a measure of trust or confidence in an authentication mechanism in terms of four levels, per the [FICAM Roadmap](#). An agency should refer to [SP 800-63](#) for the technical requirements and guidance for each of the four levels of assurance. An agency should also refer to [Office of Management and Budget Memorandum 04-04 \[OMB M-04-04\]](#) which requires agencies to review new and existing electronic transactions to ensure authentication processes provide the appropriate level of assurance. This is particularly important as an agency manages its provisioned privileged users during Run-Time Access Control.

<sup>43</sup> See Section 8 of the [FICAM Roadmap](#) for more information around the PIV-Interoperable (PIV-I) card.



Once a privileged user has been issued a credential and assigned elevated access during Provisioning, additional security controls are required to manage his/her access to protected resources, which are described in the following sections.

### 3.3. Run-Time Access Control

Once the privileged user successfully completes Provisioning (Section 3.2), the Run-Time Access Control element of the framework enforces authentication and authorization when he/she makes an access attempt. These activities are preventive controls to determine that the use of elevated access is appropriate. Several access controls models (e.g., Role-based Access Control, Attribute-based Access Control, Risk-adaptable Access Control)<sup>44</sup> exist for implementing this portion of the framework. An agency can find guidance on selecting the appropriate access control model in The Access Management Framework.<sup>45</sup>

The following table defines the protected resources a privileged user could attempt to access.

Protected Resource	Definition
<b>Data and Content</b>	<b>Data:</b> A subset of information in an electronic format that allows it to be retrieved or transmitted between different systems. <sup>46</sup>
	<b>Content:</b> Data in a usable form for one or more purposes.
<b>Applications and Web Services</b>	<b>Applications:</b> Software programs hosted by an information system that performs specific functions. <sup>47</sup>
	<b>Web Services:</b> Software systems designed to support interactive and automated interaction with information systems over a network. <sup>48</sup>
<b>Networks and Infrastructure</b>	<b>Network:</b> Information system(s) implemented with a collection of interconnected components. <sup>49</sup>
	<b>Infrastructure:</b> The hardware, storage, servers, and data center space or network components that provide IT services to an organization. <sup>50</sup>
<b>Facilities</b>	All buildings and structures occupied by Federal employees (includes existing owned, to be purchased or leased facilities; stand-alone facilities; Federal campuses; individual facilities on Federal campuses; and special-use facilities).

**Figure 4: Protected Resource Definitions<sup>51</sup>**

The privileged user's attempt to execute activities that require elevated access for the identified protected resource initiates the following processes:

- **Authentication.** The privileged user will authenticate using the required multi-factor authentication, as illustrated in Figure 2 . Multi-factor authentication involves three

<sup>44</sup> Please refer to the [FICAM Roadmap](#) section 9.3.1 and Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014 for further information on managing users with different access control models.

<sup>45</sup> Refer to the AMF for a more detailed discussion on the various access control models. (pending hyperlink)

<sup>46</sup> Adapted from [NIST IR 7298](#), Glossary of Key Information Security Terms, May 2013. [NIST IR 7298]

<sup>47</sup> As defined in [NIST IR 7298](#).

<sup>48</sup> Adapted from [W3C Web Services Glossary](#), February 2004.

<sup>49</sup> As defined in [NIST IR 7298](#).

<sup>50</sup> Adapted from [Information Technology Infrastructure Library \(ITIL\) Glossary of Terms, Definitions, and Acronyms](#), May 2007.

<sup>51</sup> Additional information regarding the protected resources can be found in the AMF.

distinct types of authentication factors: a) something you have, in this case, a PIV card; b) something you know, knowledge of the Personal Identification Number (PIN) to access protected areas of the PIV card; and c) something you are, cardholder fingerprint match with biometric data stored on the card. The confidence of the authentication increases with the number of factors used.<sup>52</sup> Based upon the level of authentication required, the privileged user will validate his/her identity through a combination of something he/she has, knows, and is.

### Implementation Tip

In a Microsoft enterprise environment, an agency may manage its privileged users' logical access by mapping each user's PIV card to multiple accounts (e.g. enable altSecurityIdentities and Username Hints). After the privileged user presents his/her PIV card at log-in, the user can specify to which valid account he/she would like to authenticate. This function provides a standard log-in experience but also secure separation between standard accounts and those requiring elevated access (i.e., privileged accounts).



- **Authorization.** Following successful authentication, the privileged user's attempted access is confirmed by the system that it is allowable. Authorization is the process of granting or denying specific access requests for obtaining and using information processing services or data and entering specific physical facilities.<sup>53</sup> Through an established access control policy, the privileged user's set of privileges, or elevated access profile, is evaluated in order to make and enforce a decision.<sup>54</sup> It is important for an agency to determine how tightly to control authorization decisions for privileged user requests to access protected resources. Management may become cumbersome for an agency if controls are too stringent or granular. Therefore, an agency needs to balance the complexity of the authorization process against the user's ability to effectively perform his/her job.

### Implementation Tip

For protected resources that do not support PIV authentication, an agency can use a privileged access gateway to enable use of the PIV card. A privileged access gateway is an intermediary between privileged users and protected resources that acts as a security checkpoint, providing authentication and authorization, as well as on-going monitoring capabilities. A privileged user authenticates to the privileged access gateway using his/her PIV card. Then, the privileged access gateway provides run-time access control to protect the resource based on the user's provisioned access and the agency's security policies. Although an agency should opt for PIV authentication where possible, PIV authentication by proxy through single sign-on does qualify as PIV-enabled, per the FY14 Chief Information Officer Federal Information Security Management Act (FISMA) Reporting Metrics.<sup>55</sup>



<sup>52</sup> [SP 800-116](#), A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), NIST, November 2008. [SP 800-116]. SP 800-116 specifies several authentication mechanisms using the PIV card to establish confidence in the identity of the cardholder. A list of authentication mechanism combinations can be found in Appendix C of SP 800-116.

<sup>53</sup> As defined in the [FICAM Roadmap](#).

<sup>54</sup> For more information regarding policy execution for access control, please refer to the AMF.


<sup>55</sup> [FISMA Metrics](#)



### 3.4. On-Going Monitoring

As an agency leverages preventive and detective measures to observe privileged user activities, there are a variety of mechanisms an agency can leverage to assist in the continuous tracking and auditing of these actions.<sup>56</sup> Maintaining an audit trail facilitates tracking of a privileged user's account(s), access entitlements, and activity across protected resources. The list below highlights key monitoring activities that assist an agency in safeguarding the enterprise.<sup>57</sup>

- **Training and Education.** Enforcing curriculum-based training is a preventive measure that can enhance employee vigilance of security protocol. As a detective measure, an agency can use training and education to develop observation skills to enhance both employee vigilance and reporting of suspicious behavior. Furthermore, an agency should hold on-going training sessions to reinforce the technical competencies commensurate to a privileged user's elevated access. An agency should maintain accurate records of these training sessions to monitor their scope and effectiveness.

Lesson Learned	
It is important for an agency to have mandatory training requirements for privileged users on a recurring basis. The State Department requires privileged users to attend a five day training class specific to their user population's role. Curriculum that reinforces the efficient and secure way to carry out assigned duties for privileged users can mitigate unwanted behavior stemming from ignorance.	

- **Access Recertification.** Renewing the privileged user's certification on a recurring basis assists in validating the need for the individual's elevated access. For example, recertification may be required on a monthly basis for a highly sensitive protected resource. Access should be removed (i.e., de-provisioned) in the event that recertification is not completed in a timely manner or if there is no longer a business need for the privileged user to have such access.
- **Session Monitoring and Anomaly Reporting.** Recording and analyzing patterns of privileged user behavior assists in identifying activity that deviates from the established baseline of normal behavior. For example, assigned job duties may require a privileged user to perform a pre-determined activity with specific steps on a daily basis by accessing a protected resource. If session recording captures the privileged user taking extraneous steps or inexplicably repeating the pre-determined activity, further investigation would be warranted. Privileged users' awareness of session recording serves to deter misuse or abuse. For privileged user activities/accounts that are highly sensitive, an agency can opt to implement live session monitoring, which is a security step above session recording.
- **Alerts.** Configuring a notification system to provide timely notice of unusual and potentially dangerous activity assists the agency in its vigilance of privileged user activity. At the time an alert is received, the agency can implement necessary preventive measures to halt further activity.

<sup>56</sup> Implementation on-going monitoring controls should be executed based on an agency's risk assessment, as described in [FIPS 199](#).

<sup>57</sup> The examples discussed are not meant to serve as an exhaustive list.

- **Keystroke Logging.** Recording and logging the keys struck on a privileged user's workstation keyboard allows an agency to oversee the privileged user's activity at a granular level. Such logging identifies key word usage that may alert the agency of suspicious behavior.
- **Audit Logs and Reviews.** Documenting and reviewing a set of audit records provides an agency with documentary evidence of a sequence of activities that has occurred on its physical or logical protected resources. Through recurring analysis, an agency may identify activity that did not trigger an alert, warranting the agency to implement more stringent monitoring of privileged user activity to properly safeguard the agency's resources. Furthermore, an agency should consistently re-evaluate the scope and effectiveness of its audit review processes.

#### Implementation Tip

An analytics capability bolsters on-going monitoring activities by empowering an agency to maximize the utility of its data and log collections by offering an easy method to detect risk indicators of security violations and unwanted behavior by privileged users. Analytics support an enterprise with a platform for automatically identifying anomalies, such as rogue or orphaned accounts, segregation of duties violations, and deviations from system access and usage patterns.



- **Continuous Evaluation.** To consistently validate privileged user suitability, an agency should work closely with its personnel security office to confirm that the access level granted to the privileged user is consistent with personnel security records. Additionally, an agency should vet privileged users with background investigations on a recurring, consistent basis to protect an agency's resources from insider threat. Performing continuous evaluation on a recurring basis cultivates a proactive security culture.

#### Implementation Tip

An agency should evaluate available tools to assist in privileged user management. Continuous Diagnostics and Mitigation (CDM) is one example of a program that provides a broad spectrum of tools that enables an agency to identify privileged user risks on an ongoing basis, prioritize these risks based upon potential impact, and enable cybersecurity personnel to mitigate the most significant problems first.<sup>58</sup>



---

<sup>58</sup> Refer to the Department of Homeland Security (DHS) [website](#) for more information regarding CDM.

## Appendix A: Reference Documentation

### ***National Insider Threat Policy***

The Presidential Memorandum of 21 November 2012 announced the Obama Administration's National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,<sup>59</sup> here forward referred to as NITP. The purpose of the NITP is to guide the executive branch in instituting effective insider threat programs, as mandated of all agencies with access to classified information in E.O. 13587.<sup>60</sup> The NITP establishes common expectations to assist executive branch agencies in benchmarking their insider threat programs. Benchmarking allows agencies to identify areas for improvement in maturing their respective insider threat mitigation programs and share lessons learned. The NITP requires federal agencies to monitor user activity on classified computer networks controlled by the Federal Government, evaluate personnel security information, provide insider threat awareness training, and gather information for a centralized capability to analyze, report, and respond to insider incidents as appropriate.

The NITP demarcates broad areas from which executive branch agencies should gather information to develop an advanced information integration capability to deter, detect, and mitigate the risk of insider threat. However, agencies require a level of granularity to inform the implementation of their respective insider threat programs. Agencies should identify specific data elements within the larger areas presented in the NITP to determine the constitution of an employee's insider threat risk profile within that agency. These data elements should be integrated appropriately to reveal the relative risk of individuals in the agency's workforce. Notably, the level of access granted to a user is critical to developing the user's insider threat risk profile: the consequence of an insider incident where the insider has elevated access to information can be greater than an incident where the insider's access to information is more limited. Therefore, an agency should prioritize information on privileged user access as data elements in calculating the relative risk of insider threat.

### ***National Strategy for Information Sharing and Safeguarding***

*The National Strategy for Information Sharing and Safeguarding*<sup>61</sup> (NSISS) was signed by the President on December 19, 2012 and contains three principles, five goals (with sub-goals), and 16 priority objectives. Goal #4 within NSISS focuses on identifying, preventing, and mitigating insider threats to the Federal Government across security domains. Additionally, related to ICAM, Priority Objective #4 calls to "Extend and Implement the FICAM Roadmap across all security domains." Given the requirements within NITP for classified networks and systems, a holistic understanding of the associated ICAM requirements is important as an agency seeks to efficiently manage its privileged user population.

Priority Objective #4 calls for the implementation of FICAM on each of the three security fabrics: Unclassified, Secret, and Top Secret. Implementation plans will be developed for each:

---

<sup>59</sup> [NITP](#), National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Presidential Memorandum, November 2012 [NITP]. For more information on the National Insider Threat Task Force (NITTF) refer to [ncix.gov](#).

<sup>60</sup> [E.O. 13587](#), Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011. [E.O. 13587]

<sup>61</sup> [National Strategy for Information Sharing and Safeguarding \(NSISS\)](#), Executive Office of the President (EOP), December 2012.

- **The Unclassified Implementation Plan** includes all Unclassified, Sensitive but Unclassified (SBU), and Controlled Unclassified Information (CUI) systems within the Executive Branch of the Federal Government and all systems and users that interact with these federal systems.
- **The Secret Implementation Plan** includes all systems within the Executive Branch of the Federal Government that process secret information and all systems and users that interact with these federal systems.
- **The Top Secret Implementation Plan** includes all systems within the Executive Branch of the Federal Government that process top secret information and all systems and users that interact with these federal systems.

As an agency works to extend its ICAM implementations across security domains, it is important to consider Goal #4 and PO #4 in relation to managing privileged users.

### ***Executive Order 13587***

The President issued *Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*<sup>62</sup> to address vulnerabilities in computer networks so federal agencies can share and safeguard classified information in a secure manner, while upholding protections for privacy and civil liberties. E.O. 13587 creates new offices and committees, while leveraging existing positions, like agency heads, to provide mechanisms and accountability measures for ensuring that policies, standards, and guidance are created that address both internal and external security threats and vulnerabilities regarding classified information both within and outside the Federal Government. E.O. 13587 requires all federal agencies that operate or access classified information or computer networks to implement an insider threat detection and prevention program, consistent with the policies developed by the National Insider Threat Task Force (NITTF), as established in E.O. 13587.

### ***Executive Order 12968, as amended***

*Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*,<sup>63</sup> the 2008 amendment of *Executive Order 12968 – Access to Classified Information*,<sup>64</sup> aligns the Federal Government’s personnel security clearance processes into a unified structure. This structure supports efforts to maintain relevant information housed by an agency in a manner that can be shared rapidly across the executive branch. E.O. 13467 empowers the Director of National Intelligence (DNI) to administer the clearance process across the executive branch, including the creation of government-wide policies on the security clearance, investigation, and adjudication processes.

---

<sup>62</sup> [E.O. 13587](#)

<sup>63</sup> [E.O. 13467](#), Executive Order 13467 – Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 2008. [E.O. 13467]

<sup>64</sup> [E.O. 12968](#), Executive Order 12968 – Access to Classified Information, August 1995. [E.O. 12968]

Additionally, E.O. 13467 authorizes the continuous evaluation of federal employees and contractors holding security clearances using automated procedures executed by a government-wide computer system thus strengthening the reciprocity of security clearances, allowing cleared personnel from one federal agency to operate more easily within another federal agency. This facilitates cooperation and resource-sharing among federal agencies involved in matters of national security, but expands the scope of insider threat at one agency to all agencies. Although automated continuous evaluation can assist in mitigating government-wide exposure to the threat posed by a single insider, E.O. 13467 reinforces the need for coherent and effective government-wide policy on privileged user access.

### ***Executive Order 10450, as amended***

E.O. 12968 aims to streamline the clearance process, while *Executive Order 10450 – Security requirements for Government employment*,<sup>65</sup> amended by several subsequent E.O.s, formally establishes the need for federal agencies to vet their employees in the first place. E.O. 10450 requires that all federal agencies conduct investigations of its employees to determine if their employment by the United States is consistent with national security interests. E.O. 10450 calls for federal agencies to gauge the suitability of its workforce for federal employment by investigating activities that reveal the employee or candidate to be untrustworthy, disloyal, criminal, unreliable, subject to coercion, or possessing malicious intent. E.O. 10450 requires that federal agencies use the mandatory investigations to protect against the intentional, unwanted disclosure of security information by agency employees. Logically, it follows that federal agencies not only implement investigative measures that prevent or uncover dangerous employees guilty of, or prone to, the aforementioned security violation, but implement role-based access control measures that deter, detect, and mitigate the effects of malicious employees.

### ***Federal Information Security Management Act***

The *Federal Information Security Management Act* (FISMA) requires all federal agencies with over 100 full time employees to continuously monitor information related to security across the enterprise. This information must be analyzed using an automated capability to help agencies manage their resources so they can effectively address vulnerabilities and threats. The goal of FISMA is to foster greater understanding of an agency's security information infrastructure with the ultimate goal of improving the federal cybersecurity defensive posture.

To that end, FISMA provides federal agencies with metrics for compliance with cybersecurity best practices: *FY2014 Chief Information Office Federal Information Security Management Act Reporting Metrics v2.0*.<sup>66</sup> Cybersecurity relies heavily on the role of the privileged user, thus privileged user management features prominently in the FISMA metrics.<sup>67</sup> FISMA stresses not only robust controls over privileged user network access, but also employee training informed by the heightened threat that privileged users pose by simple virtue of their elevated access. FISMA

---

<sup>65</sup> [E.O. 10450](#), Executive Order 10450 – Security requirements for Government employment, April 1953 (amendments included). [E.O. 10450]

<sup>66</sup> [FISMA Metrics](#), FY2014 Chief Information Office Federal Information Security Management Act Reporting Metrics v2.0, January 2014. [FISMA Metrics]

<sup>67</sup> FISMA metrics are derived from Administration Priorities (AP,) as determined by the National Security Staff and the Office of Management and Budget (OMB), baseline practices pulled from the National Institute of Standards and Technology (NIST), and metrics from FISMA itself, known as Key FISMA Metrics (KFM), revolving around six performance areas.



recognizes that an attack executed by, or directed at, a privileged user can have especially damaging effects on a federal agency. Consequently, through its mandated reporting requirements, FISMA encourages federal agencies to influence the behavior of their privileged users, whether through technical controls or training programs.

## **FIPS 199**

The *Standards for Security Categorization for Federal Information and Information Systems* (FIPS 199)<sup>68</sup> offers structure around assessing the risk surrounding information and information systems employed by the Federal Government. These common standards provide the Federal Government with an effective means of not only managing a wide array of information security programs, but facilitating security coordination among these programs. FISMA mandates the standards presented in FIPS 199 are applied to all information within the Federal Government that is not classified or belonging to a national security information system. FIPS 199 requires federal agencies rate the potential impact of a security breach on the organization or individuals. In an effort to standardize, FIPS 199 presents agencies with a matrix of the potential impact (low, medium, high) and the three security objectives defined by FISMA: confidentiality, integrity, and availability.

A privileged user has the ability to compromise all three of the core elements of information security presented in FIPS 199. Privileged users are responsible for the availability of information as they assign profiles and apportion privileges to the pool of users with standard access. Moreover, privileged users manage the integrity of the information. A privileged user has the power to irrevocably modify or delete information, creating an obvious risk for the organization and the public at large. Lastly, privileged users guard the confidentiality of information. This necessitates privilege users' access to an agency's restricted information, because these individuals must administer rights to the information. As a result, a privileged user can violate the authorized restrictions on data availability by exploiting his/her elevated access to unlawfully disclose content. The information security priorities presented in FIPS 199 demonstrate the urgency for federal agencies to not only estimate the potential consequence of an information security breach, but implement measures to mitigate those users that have been allocated extra levels of control within their computer systems. These extra levels of control endanger the three security concerns at the core of the FIPS 199 standards.

## **Federal Identity, Credentials, and Access Management (FICAM) Roadmap and Implementation Guidance**

The *FICAM Roadmap and Implementation Guidance Version 2.0*<sup>69</sup> was released on December 2, 2011. This document consists of two components: Part A and Part B.

Part A provides the ICAM segment architecture which outlines a cohesive target state to provide clarity and interoperability across agency-level initiatives. These initiatives include streamlining the collection and sharing of digital identity data, fully leveraging PIV card and PIV card-I credentials, modernizing Physical Access Control Systems (PACS) and Logical Access Control

---

<sup>68</sup> [FIPS 199](#), Standards for Security Categorization for Federal Information and Information Systems, April 2004. [FIPS 199]

<sup>69</sup> [FICAM Roadmap](#)

Systems (LACS) infrastructure, and implementing a federated identity capability. Part B provides guidance on a broad range of topics to enable a holistic approach for alignment with the ICAM segment architecture, including:

For supplemental information to assist an agency in managing its privileged users, refer to the use cases in Part A of the Roadmap (e.g., 4.7 Provision and De-provision User Account for an Application) and Section 9.2 Privilege Management. Section 9.2 of the Roadmap discusses the impacts of the ICAM segment architecture on traditional privilege management processes and introduces the automated provisioning capability that is outlined in the target state. Additionally, it discusses:

- Steps and activities that are involved in managing privileges throughout the access management lifecycle;
- Privilege management processes that may be improved by correlating similar information and access needs into defined roles; and
- The automated provisioning capability and the benefits this approach provides over current techniques.

### ***NIST SP 800-53***

In an effort to address the growing body of legislative and executive requirements on the security and privacy of information housed in federal systems, the National Institute of Standards and Technology (NIST) released a special publication in April 2013, Security and Privacy Control for Federal Information Systems and Organizations (SP 800-53).<sup>70</sup> By providing a holistic and integrated approach to information security in the federal space, this document provides agencies with the fundamentals of implementing robust, risk-based cybersecurity programs. SP 800-53 stresses that agencies have flexibility in the manner of they implement security controls; however, the document has additional salient themes. Notably, of the multitude of security controls included in SP 800-53, dozens revolve around restricting and properly monitoring the accounts and access of privileged users. These controls range from exercising the rule of least privilege to ensuring information integrity.

### ***Common Sense Guide to Mitigating Insider Threats (4th Edition)***

The Software Engineering Institute at Carnegie Mellon University's Insider Threat Center released the *Common Sense Guide to Mitigating Insider Threats (4th Edition)* (Common Sense Guide)<sup>71</sup> in December 2012 to provide the Federal Government and industry with recommendations on insider threat mitigation, based on a database of over 700 cases. This work was sponsored by the Department of Homeland Security, Office of Cybersecurity and Communications and the U.S. Secret Service.

The Common Sense guide presents readers with 19 best practices to mitigate insider threats within organizations, with accompanying case studies for each. Practice 10 involves instituting stringent access controls and monitoring policies on privileged users. Due to privileged users'

---

<sup>70</sup> [SP 800-53](#), Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, NIST, April 2013. [SP 800-53]

<sup>71</sup> [Common Sense Guide to Mitigating Insider Threats \(4th Edition\)](#), CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University, December 2012. [Common Sense Guide]

elevated access, cases of insider threat involving these individuals often have a significant impact on organizations. As a result, case studies for the other 18 best practices listed in the Common Sense Guide prominently feature privileged users.



## Appendix B: Classifications of Insider Threats and Privileged Users

In recent years, privileged users within agency boundaries have inflicted harm on the Federal Government through the misuse or abuse of the elevated access granted to them. The administrative and security functions commonly assigned to privileged users require this elevated access, yet it renders privileged users inherently risky because of their potential to jeopardize agency resources, either knowingly or unknowingly. Therefore, privileged user management is an important element of insider threat mitigation. In improving privileged user management capabilities, an agency is simultaneously building up its protection against insider threat.

Understanding how privileged user management fits into the insider threat landscape enforces the Privileged User Management Framework. Not only do a variety of user types and accounts typically comprise an agency's privileged user population, but the basis of these privileged users' potential for unwanted behavior (Figure 1) can vary. In an effort to appropriately manage its privileged user population, an agency should be aware of three different classifications of insider threat, because the more intentional insider activity, the more difficult it can be to detect and mitigate. These classifications apply to an organization's entire workforce, with its privileged user population existing as a subset of that. An agency can do a number of things to mitigate these three classifications of insider threat, all of which are contained in the Privileged User Management Framework:

- **Training and Education** - (Section 3.4) can primarily prevent the insider threat stemming from accidental behavior, but heightened security awareness can mitigate complacent insiders as well.
- **Internal Controls** - (Sections 3.1, 3.2, 3.3), like segregation of duties, can mitigate insider threat stemming from accidental and complacent behavior.
- **On-going Monitoring Capabilities** - (Section 3.4) can mitigate the insider threat posed by the often deceptive malicious insider. However, as the most sophisticated measure to insider threat, on-going monitoring empowers an agency to mitigate all three classifications of insider threat at once, as this can deter and detect security violations by accidental and complacent insiders, as well as malicious ones.

The following table presents the three classifications of insider threat with accompanying examples of how specifically privileged users of each classification can pose a threat to an agency.

Classifications of Insider Threats	Definition	Indicators	Examples of Privileged User Insider Threats
<b>Accidental</b>	An insider's lack of awareness regarding policies, procedures, and technical competencies results in a security risk for the organization.	An insider lacks an understanding of security protocols, technical procedures, and the potential impact of deviating from an organization's security protocol and the individuals assigned job duties.	<ul style="list-style-type: none"> <li>• A privileged user unknowingly installs software that is not approved for use on an agency system.</li> <li>• Use privileged accounts for anything other than official administrative actions.</li> <li>• A privileged user accidentally deletes all data with a single command.</li> </ul>

Classifications of Insider Threats	Definition	Indicators	Examples of Privileged User Insider Threats
<b>Complacent</b>	An individual or organization's lax approach to security causes an insider to neglect security obligations, despite his/her awareness of protocol.	Violating insider assumes his/her behavior does not have a noticeable impact or that it is not being monitored. Over time, the insider becomes careless with security.	<ul style="list-style-type: none"> <li>Privileged users create user accounts and assign privileges without the appropriate review and approval.</li> <li>Privileged users share passwords to system accounts.</li> </ul>
<b>Malicious</b>	Personal circumstances or specific events lead an insider to intentionally disrupt, threaten, or endanger an organization's activities or assets.	Insider usually develops a plan to breach security in advance. Insider typically exhibits behavior, virtual or in person, that is unusual for the insider's personality or job duties.	<ul style="list-style-type: none"> <li>Unwanted, purposeful disclosure or theft of information.</li> <li>Introduce malicious code, malware, Trojan horse, viruses into the organization's information system.</li> <li>Destroy or modify system audit logs.</li> </ul>

**Figure 5: Classifications of Insider Threat and Privileged Users**

Understanding insider threat classifications supports an agency's implementation of the Privileged User Management Framework (Section 3), as the measures contained within the framework operate in unison to mitigate the range of privileged users' basis for unwanted behavior. Furthermore, the relationship between the three insider threat classifications and the Privileged User Management Framework aids an agency in the broader effort of fulfilling the insider threat mitigation requirements in the NITP and relevant Executive Orders.

These classifications are discussed throughout Appendix C: Privileged User Security Controls Mapping for Special Publication 800-53 in the "Explanation" column. This allows an agency to further integrate relevant controls for privileged user management with insider threat mitigation efforts.

## Appendix C: Privileged User Security Controls Mapping for Special Publication 800-53

In seeking to implement cohesive, integrated privileged user management practices (e.g., Secure Operating Environment, Provisioning, Run-Time Access Control, On-Going Monitoring) via the Privileged User Management Framework, an agency should consider existing controls and practices which can assist in safeguarding the enterprise's protected resources from privileged user insider threats. This section provides an analysis of countermeasures for privileged user misuse and abuse of elevated privileges by leveraging SP 800-53.<sup>72</sup> SP 800-53 provides a general framework for applying security controls to any federal information system, regardless of its mission. The following subsections augment the controls defined in SP 800-53 into countermeasures. In addition to the framework in Section 3, these countermeasures can assist an agency in mitigating unwanted behavior by its privileged user population through providing a complementary set of security controls specific to privileged users' security and administrative functions. This type of supplemental control specific to a particular community or system type is allowed per SP 800-53 and within this document is referred to as a mapping.

For each identified countermeasure, an accompanying explanation provides guidance on how the associated control relates to privileged users to assist an agency defend relevant protected resources.<sup>73</sup> The controls are organized into the control families as listed in SP 800-53. The countermeasures can be applied as security measures in accordance with an agency's protected resource analysis (Section 2.1).

### Access Control

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Manage privileged user accounts</b>	AC-2	Management of users that have been granted elevated access requires additional scrutiny by agency personnel. Privileged user accounts can be managed through a variety of ways, including: <ul style="list-style-type: none"> <li>• Appropriate approval mechanisms based on mission and business functions</li> <li>• Clear identification of roles and responsibilities</li> <li>• Access attributes (i.e., timeframes, point-of-origin)</li> <li>• Timely issuance and revocation process for credentials based on established timeline or event (i.e., individual is removed from group)</li> <li>• Continuous evaluation of access needs</li> </ul>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Institute separation of duties for privileged users</b>	AC-5	Separation of duties does not guarantee that privileged users will not abuse or misuse their elevated access, but it can mitigate the risk of an individual privileged user inflicting harm. By dividing the mission functions and information system support performed by privileged users among a pool of individuals or accounts, an agency can work to	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>

<sup>72</sup> This analysis is not meant to be exhaustive; however, is intended to assist an agency in correlating practices to existing controls. Refer to [SP 800-53](#).

<sup>73</sup> Refer to Section 3.3 for the definitions of each protected resource highlighted in the privileged user management lifecycle.

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
		mitigate one privileged user from amassing too much power or undermining monitoring activities. In particular, an agency should confirm the same individuals do not administer both access control and audit functions. An agency should document how its individual privileged users are segregated throughout the agency.	
<b>Exercise the principle of least privilege for information systems</b>	AC-6	<p>The principle of least privilege involves confirming an agency's privileged users are only granted access to the information systems required to carry out each individual's specific job duties. It is an important countermeasure to mitigating unwanted behavior by privileged users.</p> <ul style="list-style-type: none"> <li>Least privilege is particularly important regarding the management of privileged users, as their elevated access already greatly increases the consequence of their actions and impact on protected resources.</li> <li>Privileged users can accumulate authorizations as they transition from projects and departments. The failure to conduct continuous evaluation activities and terminate excess privileges as appropriate renders these privileged users a security risk. Such individuals can cause harm to an agency, knowingly or unknowingly.</li> </ul>	<ul style="list-style-type: none"> <li>Applications and web services</li> <li>Network and infrastructure</li> </ul>
<b>Secure remote access for privileged users</b>	AC-17	<p>Remote access points such as dial-up, broadband, and wireless, can be complex to monitor (e.g., VPNs with encrypted tunnels). Certifying privileged users are subject to stringent access controls and monitoring is thus especially important with remote access. Privileged users should not be able to act remotely the same way they do when they access the network locally. An agency can protect the enterprise from the privileged user insider threat via remote access by:</p> <ul style="list-style-type: none"> <li>Limiting the execution of privileged commands and access for a narrowly defined subset of needs</li> <li>Establishing stringent connection requirements and session controls (e.g., session duration limitations, automatic termination when user is idle)</li> <li>Instituting a remote monitoring and intervention capability</li> </ul>	<ul style="list-style-type: none"> <li>Applications and web services</li> <li>Network and infrastructure</li> </ul>

**Figure 6: Access Control**

## Awareness and Training

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Conduct security awareness training on the threat privileged users can pose</b>	AT-2	Agencies should work to ensure that privileged users who access information systems receive security awareness training on the role everyone plays in maintaining security, and insider threat training should be a component of this. Not only does this training bolster an agency's insider threat detection capabilities, but it serves as a deterrent for individuals who consider abusing the access granted to them. A training module is a fitting venue to discuss the inherent risk posed by privileged users.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and Web Services</li> <li>• Networks and Infrastructure</li> <li>• Facilities</li> </ul>
<b>Institute role-based security training for privileged users</b>	AT-3	<p>An agency should train privileged users on proper security protocol based on their job duties. Training is a preventive method for protecting the enterprise against accidental insiders. This is especially important for privileged users, because the consequence of their abuse or misuse on protected resources can be greater than users who do not have elevated access.</p> <p>Individuals tasked with overseeing physical security controls require different specialized training than database administrators, for example. The agency should confirm each privileged user has received adequate technical training based on assigned duties and the protected resources they are each responsible for.</p>	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and Web Services</li> <li>• Networks and Infrastructure</li> <li>• Facilities</li> </ul>

Figure 7: Awareness and Training

## Audit and Accountability

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Determine the pool of audit events</b>	AU-2	<p>A primary component of an agency's ability to manage its privileged user population is an audit capability using a log correlation engine or security information and event management (SIEM) that can monitor employee activities. An agency needs to determine the scope of audit events, but should work to ensure that all types of privileged users are adequately monitored. When determining the pool of audit events, all departments within the agency should be engaged to leverage all audit-related information in order to generate a comprehensive picture of an employee's relative risk. Audit events can include:</p> <ul style="list-style-type: none"> <li>• Password changes</li> <li>• Failed access attempts related to information systems</li> <li>• Administrative privilege usage</li> <li>• Secure credential usage (e.g., PIV card, CAC, third-party)</li> </ul>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Use adequate audit records</b>	AU-3	<p>Audit records that contain vague information or that lack adequate event details are ineffective in assisting an agency in managing its workforce. Audit records should include:</p> <ul style="list-style-type: none"> <li>• Type of event</li> <li>• Time of the event</li> <li>• Location of event</li> <li>• Source of event</li> <li>• Outcome of event</li> <li>• Identity of individuals involved with event</li> </ul> <p>Not all auditable events can be audited at the same time, so the agency should determine under which circumstances events are audited. It should be noted that audit records for privileged user activity that come with the computing platform are often inadequate, and require refining.</p>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>
<b>Set up processes to review, analyze, and report on auditing records</b>	AU-6	<p>Auditing components such as account usage, remote access, and configuration settings allow an agency insight into whether its privileged users are abiding by security protocol.</p> <p>An agency can improve its ability to mitigate the threat posed by privileged users through enhancing the auditing capability's integration and correlation with other processes like physical monitoring, non-technical sources, and vulnerability scanning. Full-text analysis of privileged commands can greatly improve an agency's management of its privileged users and accounts.</p> <p>In particular, malicious insiders require an integrated, enterprise-wide mitigation approach. To mitigate unwanted behavior by malicious privileged users, an agency should consider feeding its auditing information into an analytic capability.</p>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>
<b>Protect audit information from unwanted changes</b>	AU-9	<p>An agency should take technical measures to protect its audit resources (e.g., settings, records, and reports), such as limiting access. The management of audit resources inherently requires elevated access. A privileged user insider with nefarious motives may have incentive to tamper with an agency's audit capabilities. A privileged user that is subject to the auditing processes and also has the means to alter audit resources poses an intrinsic risk of manipulation. An agency can dedicate a subset of privileged users to manage the audit functions to improve reliability of the audit capabilities.</p>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>

**Figure 8: Audit and Accountability**



## Security Assessment and Authorization

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Establish Interconnection Security Agreements where necessary</b>	CA-3	Weak governance of system interconnections can create an opportunity for insiders to exploit information systems and exfiltrate data without authorization, particularly those with privileged access. Because different systems may have different security requirements, authorizing officials should establish Interconnection Security Agreements that document the interface characteristics, security requirements, and nature of the information communicated. If the rules of system interconnection are clearly defined, accidental and complacent insider activity by privileged users who manage these systems can be avoided to some extent, while malicious insider activity by privileged users also in this role can be deterred or detected more easily.	<ul style="list-style-type: none"> <li>• Network and infrastructure</li> </ul>

Figure 9: Security Assessment and Authorization

## Configuration Management

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Develop and maintain configuration baselines for information systems</b>	CM-2	By establishing baseline configurations for information systems and their components, an agency can help prevent privileged users from incorrectly assuming a role in altering the information system. Even though baseline configurations must change over time to reflect the current enterprise architecture, this countermeasure centralizes information about the information system components and network topology. This centralization can delineate parameters around the role of privileged users to provide guidance on configurations management so the system performs as intended. Documenting the configurations of all assets allows the agency to audit for anomalies, possible signs of insider activity from the privileged users in relevant roles.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Change configuration baselines in a secure, systematic manner</b>	CM-3	Unwanted changes to configuration baselines can create severe vulnerabilities for information system components. An agency should use Configuration Change Boards to approve major changes to the baseline configuration to reflect the current enterprise architecture. Since this is a privileged function, changes should be conducted by a group of people to maintain accountability and avoid abuse by one individual. An agency should have a clearly defined system of proposal, justification, implementation, testing, review, and disposition for system upgrades and modifications.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Appropriately restrict privileged users' ability to modify information systems</b>	CM-5	An agency should limit the privileges for modifying the hardware and software or firmware components of an information system because these changes have such a significant impact on the security of protected resources. The individuals who perform these duties are privileged users because of these changes require elevated access. An agency should maintain access records to confirm these privileged users appropriately carry out their duties. In addition, an agency can institute processes like dual authorization and code authentication for installed components to restrict the privileged users' ability to misuse or abuse their trusted position of modifying the information system.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>
<b>Establish, document, and monitor configuration settings</b>	CM-6	An agency needs to establish and document configuration settings, as well as record deviations from the agreed upon security parameters for the various information systems within the organization. Once the security parameters are defined and documented, an agency is positioned to monitor configuration changes to ensure that the privileged users tasked with configuration duties are adhering to agency policies.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Ensure information system components are fitted for least functionality</b>	CM-7	By limiting functionality of information system components to only those that are necessary, an agency can protect the enterprise against unwanted data exfiltration by employees. For example, physical or logical ports, fire-sharing capabilities, or instant messaging can be disabled when the component does not require its use. An agency can employ blacklisting (list of unwanted software) or whitelisting (list of authorized software) to further inhibit unwanted actions. Implementing these controls allows the agency an extra layer of protection against abuse or misuse of its systems by privileged users, as well as standards users.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Create a centralized inventory of information system components</b>	CM-8	Implementing a centralized information system component inventory allows an agency to hold its privileged users accountable. Hardware inventory specification, software license information, software version numbers, and component owners should be well documented. When a privileged user transitions within the organization or is granted additional access, the individual may accumulate entitlements, licenses, or components that they do not need for his/her assigned duties. This can create an opportunity for abuse or misuse and undermine monitoring activities. With a centralized inventory, an agency can protect itself against unwanted components, ensure components are properly administered, and avoid duplicate accounting of components. An understanding of an organization's assets is an important element of insider threat mitigation, especially in regards to the privileged users tasked with administration and security functions for these information system components.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>

**Figure 10: Configuration Management**



## Contingency Planning

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Use an alternate storage site</b>	CP-6	An alternative storage site for information system backup information, geographically distinct from the primary site, increases complexity for a malicious privileged user to purposefully inflict damage on an agency. By housing information in two or more distinct places, an individual would have to destroy or modify the information housed in both sites to permanently cripple the information system's backup capabilities. An agency should carefully monitor and implement stringent processes for the privileged users who have access to both sites.	<ul style="list-style-type: none"> <li>Content and data</li> </ul>
<b>Back up information system data appropriately</b>	CP-9	As part of an agency's contingency plan, user-level, system-level, and security-related documentation should be backed up using digital signatures, cryptographic hashes, etc. Backing up information can prevent the unwanted destruction or modification of information. An agency should consider implementing dual authorization mechanisms for the privileged users that manage this backup data.	<ul style="list-style-type: none"> <li>Applications and web services</li> <li>Network and infrastructure</li> </ul>
<b>Restore information systems following failures and conduct post-recovery assessments</b>	CP-10	An agency should have secure recovery processes in place if information systems are disrupted. An information system failure presents ample opportunity for a malicious privileged user to manipulate critical recovery processes tasked to him/her. An agency should conduct assessments of the information systems once fully restored to ensure all recovery processes executed by the privileged users tasked with these duties were valid.	<ul style="list-style-type: none"> <li>Applications and web services</li> <li>Network and infrastructure</li> </ul>

Figure 11: Contingency Planning

## Identification and Authentication

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Require the use of the PIV card credential</b>	IA-2	All agencies should be leveraging PIV card credentials for employee access to physical and logical resources per HSPD-12 and alignment with the ICAM target state. Information systems need to uniquely identify and authenticate its users to maintain security. However, to manage privileged users, an agency could require an additional layer of authentication, in addition to the standard multifactor authentication used for local and network access. Namely, an agency should consider implementing unique identification of individuals using shared privileged accounts and detailed accountability of individual privileged user activity.	<ul style="list-style-type: none"> <li>Applications and web services</li> <li>Network and infrastructure</li> <li>Facilities</li> </ul>

Figure 12: Identification and Authentication

## Incident Response

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Develop and implement incident handling capability commensurate to inherent risk of privileged user abuse</b>	IR-4	As part of business process development for an agency's information systems, an incident handling capability must be designed to incorporate detection, analysis, containment, eradication, and recovery. The consequence of privileged user misuse or abuse of the information system is greater than standard users because of privileged users' elevated access. As a result, privileged users may require more vigorous audit, network, and physical monitoring. The primary purpose of these robust monitoring capabilities is to enable the agency to handle security incidents effectively. As such, mitigating the insider threat posed by privileged users through incident handling is an important component to managing the privileged user population effectively. An agency can achieve effective incident handling through organization-wide coordination of mission owners, information system owners, human resources, physical and personnel security, etc.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Develop an information spillage response plan</b>	IR-9	In managing its privileged user population, an agency should work to mitigate information spillage – namely, the unwanted disclosure of information and the theft of intellectual property. This includes when, intentionally or accidentally, classified or sensitive information is placed on information systems that are unwanted to process it. Developing a secure, timely, and organized response to information spillage can mitigate the harmful effects on the agency. Since information spillage is a primary concern for agencies in regards to privileged users, developing an appropriate response plan only serves to improve an agency's privileged user management.	<ul style="list-style-type: none"> <li>• Content and data</li> </ul>

Figure 13: Incident Response

## Maintenance

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Exercise strict supervision and access procedures for maintenance personnel</b>	MA-5	<p>Maintenance personnel can be considered privileged users due to their trusted position with information systems and the extraordinary access granted to them. Software and hardware require maintenance often on short notice. As such, an agency might have to bring in individuals not previously identified as authorized maintenance personnel.</p> <ul style="list-style-type: none"> <li>• An agency should maintain a list of individuals authorized to carry out this type of maintenance.</li> <li>• For those individuals who are not escorted throughout the facility, the agency should verify</li> </ul>	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> <li>• Facilities</li> </ul>

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
		<p>these maintenance personnel have the necessary and required authorizations.</p> <ul style="list-style-type: none"> <li>For those individuals who do not possess required authorizations and must be escorted, supervisory personnel must possess the technical expertise to oversee the maintenance activities. This measure can detect or deter harmful activity on the part of the maintenance personnel.</li> <li>Temporary credentials (e.g., visitor badge, password) granted to maintenance personnel must be terminated as soon as maintenance concludes.</li> </ul>	

**Figure 14: Maintenance**

## **Media Protection**

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Restrict media use for privileged users</b>	MP-7	<p>An agency can restrict the types of media used on information systems through technical or policy-based safeguards. Prohibiting the use of writeable, portable devices or restricting the use of all media to a set of approved devices can prevent the unwanted disclosure of information, intellectual property theft, or the introduction of dangerous files or software. The restriction of media use is especially important regarding privileged users, because these users often have sweeping access to an agency's files for administrative or security purposes. Additional controls around the content and data that privileged users' access may be necessary to confirm these users' interactions with these resources are restricted to those necessary for their assigned duties.</p>	<ul style="list-style-type: none"> <li>Content and data</li> <li>Networks and infrastructure</li> </ul>

**Figure 15: Media Protection**

## Physical and Environmental Protection

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Monitor physical access of privileged users</b>	PE-6	<p>Monitoring physical access is fundamental to conducting continuous evaluation activities, which determine on an ongoing basis that all users, including privileged users, are granted the proper access to the protected resources their job roles require.</p> <ul style="list-style-type: none"> <li>Continuous evaluation is a central component to privileged user management, as the scope of these individuals' elevated access should be constantly validated because of the inherent risk of harm to protected resources.</li> <li>If an organization's physical access monitoring detects suspicious activity, like access for unusual lengths of time, the user could present an insider threat.</li> <li>Robust physical monitoring capabilities serve as a deterrent to malicious insider activity.</li> </ul>	<ul style="list-style-type: none"> <li>Networks and infrastructure</li> <li>Facilities</li> </ul>

Figure 16: Physical and Environmental Protection

## Planning

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Rules of behavior</b>	PL-4	<p>An agency should administer and collect signed agreements from all users that delineate both their responsibilities and the behavior expected of them, based on their assigned duties. This process should be completed before the user is issued a unique credential to the protected resource. In particular, these rules of behavior should differ based on the level of privilege. An agency can protect itself from unwanted behavior by privileged users through such agreements. These documents can prevent accidental and complacent privileged user insider activity, and deter malicious insider activity by communicating the severe ramifications. An agency should consider requiring a renewal of such agreements periodically (e.g., annual basis).</p>	<ul style="list-style-type: none"> <li>Content and data</li> <li>Applications and web services</li> <li>Networks and infrastructure</li> <li>Facilities</li> </ul>

Figure 17: Planning

## Personnel Security

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Develop, document, and disseminate clear policies on personnel security</b>	PS-1	An agency should monitor employees with elevated access beginning with the hiring process. In managing components of a workforce, clearly documented personnel policies are important. The privileged user should be aware of all facets of the agency's duties and abilities to determine access rights for, adjust responsibilities of, and monitor its privileged user population. This not only provides legal protection for the agency, but the ramifications of misuse or abuse serve as a deterrent to unwanted behavior by privileged users.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Assign risk designations for privileged users</b>	PS-2	An agency should assign a risk designation for all positions within the organization which will inform an individual's screening criteria and authorization procedures. As privileged users likely have the potential for adverse impact on the efficiency or integrity of the services an agency provides, <sup>74</sup> these privileged positions may warrant categorization as medium or high risk, depending on the agency's information systems, data, and the individuals' assigned duties. This risk categorization acts as tool for an agency to manage a privilege user's employee lifecycle.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Screen privileged users based on type of risk designation</b>	PS-3	Personnel screening criteria hinge on an individual's risk designation. However, an agency is free to define different screening conditions and frequencies based on the information processed, stored, or transmitted by information systems. If a user has elevated access to manage a critical information system, an agency can enforce stricter screening procedures. Screening involves coordination with personnel security (e.g., background investigation status, reinvestigation).	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Follow secure and comprehensive personnel termination procedures</b>	PS-4	Termination procedures are especially important if the departing employee had been granted elevated access, because a disgruntled, privileged user poses an even greater risk to an agency's protected resources than a disgruntled user with standard access. When terminating an employee, the agency should: <ul style="list-style-type: none"> <li>• Immediately terminate the employee's physical and logical access (i.e., PIV card, keys, system administration manuals), especially if the termination occurred under unfavorable circumstances, to prevent unwanted access to protected resources once termination is finalized.</li> <li>• Notify security personnel and the departing employees' colleagues of the departure, so these individuals do not assist the departed employee in accessing the protected resources because of their familiarity.</li> </ul>	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>

<sup>74</sup> Definition can be found in [5 C.F.R. 731.106](#).

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Continuously evaluate authorizations granted to the privileged user population</b>	PS-5	If a privileged user transfers to a different department within the agency, the individual might be granted additional physical and logical access associated with new job duties. Failing to terminate privileges from an individual's prior assignment risks inadvertently empowering the privileged user with a greater collection of authorizations than is explicitly needed. Maintaining access authorizations in line with Human Resources records is critical to mitigating the threat a privileged user can pose to an agency. An agency should conduct continuous evaluation on its privileged users to confirm these individuals have an ongoing operational need for their privileges.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Confirm employees sign access agreements prior to granting them access</b>	PS-6	Prior to granting access, an agency should develop, distribute, and document signed access agreements for employees who use agency information systems. Through non-disclosure agreements, acceptable use agreements, and rules of behavior agreements an agency can hold its employees accountable. An agency should consider tailoring these agreements to privileged users where necessary, as the nature of their access is very different than that of standard users.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>
<b>Institute a formal personnel sanctions process</b>	PS-8	Access agreements should explain the ramifications of employees violating the terms of agreement, including any personnel sanctions involved. By instituting a formal sanctions process the agency can protect its resources from privileged users who exhibit tendencies towards unwanted behavior.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>

**Figure 18: Personnel Security**

## ***Risk Assessment***

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Incorporate privileged user insider threat into enterprise-wide risk assessments</b>	RA-3	An agency should consider incorporating privileged user misuse and abuse of protected resources into its enterprise-wide risk assessments. Once critical data, systems, and business process are identified, the agency can assess the associated privileged user threats, vulnerabilities, and likelihood of an insider incident to inform the risk assessment. Please refer to Section 2.1 for more information on conducting a risk assessment as part of a protected resource analysis to identify privileged users.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Applications and web services</li> <li>• Networks and infrastructure</li> <li>• Facilities</li> </ul>

**Figure 19: Risk Assessment**

## System and Services Acquisition

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Have a robust system development life cycle</b>	SA-3	An agency needs a well-defined system development life cycle (SDLC) to verify that appropriate controls and business processes are in place to guard against privileged user abuse or misuse of protected resources. To effectively integrate these security requirements into the enterprise architecture, qualified personnel from across the organization need to work in unison. As some of these personnel may have privileged access, it is important to identify these individuals and then define and document their information security roles and responsibilities to reduce the ease of exploitation. Please refer to Section 2.1 for more information on identifying privileged users.	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Identify vulnerabilities within information systems</b>	SA-5	As part of the implementation and operation of security controls associated with information systems, known vulnerabilities regarding configuration and use of privileged functions should be identified. This knowledge allows an agency to target areas for stringent access control and monitoring of privileged users. Furthermore, these vulnerabilities can feed into the enterprise risk assessment (RA-3).	<ul style="list-style-type: none"> <li>• Applications and web services</li> <li>• Network and infrastructure</li> </ul>
<b>Require that information system developers structure for least privilege</b>	SA-17	An agency can require that internal or external developers of the information system, system component, or system service structure security-relevant hardware, software, and firmware to facilitate controlling access by least privilege. This is particularly important for privileged users, who are can be granted sweeping access to systems with a default account because this is easier than creating dozens of personalized accounts assigned to individual privileged users.	<ul style="list-style-type: none"> <li>• Network and infrastructure</li> </ul>

Figure 20: System and Services Acquisition



## System and Communications Protection

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Boundary protection</b>	SC-7	Monitoring and controlling communications at the external boundary of an information system allows an agency to develop a baseline of normal network device behavior. Using baselines, an agency can deploy anomaly detection capabilities to identify suspicious insider activity. Furthermore, an agency can opt to route networked privileged access through a dedicated interface for improved access control and auditing of users with elevated access.	<ul style="list-style-type: none"> <li>• Network and infrastructure</li> </ul>
<b>Protection of Information at Rest</b>	SC-28	An agency should implement measures to protect the confidentiality and integrity of system and user information while located on storage devices. This information can be protected through cryptographic means, file sharing scanning, etc. Since privileged users' job functions may entail performing administrative and security related functions on this information, enhanced protection increases an agency's privileged user management capabilities.	<ul style="list-style-type: none"> <li>• Content and data</li> <li>• Network and infrastructure</li> </ul>

Figure 21: System and Communications Protection

## System and Information Integrity

Countermeasure	SP 800-53 Control	Explanation	Relevant Protected Resources
<b>Internal information system monitoring</b>	SI-4	As part of formalized insider threat program, an agency should monitor its information systems for internal events. This can include real time monitoring of audit activities, access patterns, and communications traffic anomalies. The agency can define its own additional monitoring requirements for its privileged users based on its systems, mission, and business processes. However, information system monitoring is a critical component of an organization's continuous monitoring and incident response programs, and thus an integral part of privileged user management.	<ul style="list-style-type: none"> <li>• Network and infrastructure</li> </ul>

Figure 22: System and Information Integrity

## Appendix D: Privileged User Instruction

Below is an instruction template for an agency to tailor to uphold mission and business needs in support of privileged access to logical and physical resources. An agency should obtain and retain a digitally signed copy of such instruction and ensure that privileged user access to the identified protected resource is prohibited without a signed acknowledgement of system-specific rules and a signed acknowledgement of said instruction.

### [AGENCY NAME] Privileged Access User Agreement<sup>75</sup>

I am being granted elevated access to [AGENCY NAME] controlled systems and facilities and am responsible for all actions taken under my accounts. I agree to the following:

6. I will only use the elevated granted to me to perform authorized tasks or mission-related functions.
7. I will not use my elevated access to perform routine tasks that do not require elevated access.
8. I will obtain and maintain required certifications and trainings according to [AGENCY POLICY], including but not limited to specialized role-based security or privacy training.
9. I understand the need to safeguard all credentials at the level appropriate to the data they protect.
10. I will not share passwords, accounts, or other credentials with unwanted personnel.
11. I will only add and remove users to the [ADMINISTRATOR GROUPS] group after receiving approval/direction from the [AGENCY POINT OF CONTACT].
12. I will not install, modify, or remove any hardware or software without written entitlement and approval from the [AGENCY POINT OF CONTACT].
13. I will not introduce any viruses, malicious/unwanted code, malware, or Trojan horse programs into [AGENCY NAME] systems.
14. I will not attempt to hack the network or connected information systems, gain access to data or protected resources which I do not have authorized access. I will not use sensitive information for anything other than the purpose for which it has been authorized.
15. I understand that there are distinct information systems and access points – [AGENCY SECURITY DOMAINS]. I will not introduce or process data or software for information systems that I have not have elevated access to.
16. I will contact the [AGENCY POINT OF CONTACT] if I require clarification of my roles or responsibilities.

I understand that failure to comply with the above requirements may result in disciplinary action, including termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I also understand that violation of certain laws, such as

---

<sup>75</sup> Derived from documentation provided by Defense Manpower Data Center and [Health and Human Services](#)

the Privacy Act of 1974, copyright law, and 18 USC 2071 can result in monetary fines and/or criminal charges that may result in imprisonment.

---

Name

Digital Signature

Date